Comment: This is a native WP9 document.

STATEMENT BY HAROLD C. RELYEA
CONGRESSIONAL RESEARCH SERVICE
BEFORE
HOUSE GOVERNMENT REFORM
SUBCOMMITTEE ON NATIONAL SECURITY,
EMERGING THREATS, AND INTERNATIONAL RELATIONS
MARCH 2, 2005
EMERGING THREATS: OVERCLASSIFICATION AND PSEUDO-CLASSIFICATION

Mr. Chairman and members of the Subcommittee, thank you for your invitation to appear here today to offer testimony regarding the subject matter of this hearing, the emerging threats posed by overclassification and pseudo-classification of information within the federal departments and agencies. I am Harold C. Relyea, a Specialist in American National Government with the Congressional Research Service of the Library of Congress.

There can be little doubt at this late date that the terrorist attacks of September 11, 2001, have prompted rethinking and continuing concern about various aspects of the internal security — or homeland security — of the United States, not the least of which includes the public availability of information of potential value to terrorists for either the commission of their acts or forewarning them of ways of their being detected. Oftentimes, it has not been clear to what extent, if any, an attempt was made to weigh citizen needs for information vis-a-vis denying its availability to terrorists, or if thoughtful consideration was given to alternative limits short of total restriction. "At the very least," a Heritage Foundation report observed not long ago, "such wholesale withdrawal of information seems arbitrary and undermines important values of government openness, the development of electronic government (e-gov) to speed the delivery and lower the costs of government services, and public trust."[1] The recent creation of privacy and civil liberties officers and institutions may ameliorate this and other information management concerns, including the collection, security, and scrutiny of vast amounts of personally identifiable information.

---

[1] James Jay Carafano and David Heyman, "DHS 2.0: Rethinking the Department of Homeland Security," *Heritage Special Report* (Washington: Dec. 13, 2004), p. 20.

Security Classification

A primary tool for protecting information in the post-9/11 environment is the classification of national security information.[2] Current security classification arrangements, prescribed by an executive order of the President, trace their origins to a March 1940 directive issued by President Franklin D. Roosevelt as E.O. 8381. This development was probably prompted somewhat by desires to clarify the authority of civilian personnel in the national defense community to classify information, to establish a broader basis for protecting military information in view of growing global hostilities, and to better manage a discretionary power seemingly of increasing importance to the entire executive branch. Prior to this 1940 order, information had been designated officially secret by armed forces personnel pursuant to Army and Navy general orders and regulations. The first systematic procedures for the protection of national defense information, devoid of special markings, were established by War Department General Orders No. 3 of February 1912. Records determined to be "confidential" were to be kept under lock, "accessible only to the officer to whom intrusted." Serial numbers were issued for all such "confidential" materials, with the numbers marked on the documents, and lists of same kept at the offices from which they emanated. With the enlargement of the armed forces after the entry of the United States into World War I, the registry system was abandoned and a tripartite system of classification markings was inaugurated in

[2] This historical overview derives from Harold C. Relyea, "The Evolution of Government Information Security Classification Policy: A Brief Overview (1775-1973)," in U.S. Congress, House Committee on Government Operations, *Security Classification Reform*, hearings, 93rd Cong., 2nd sess. (Washington: GPO, 1974), pp. 505-597; Harold C. Relyea, "Appendix II: Government Information Security Classification Policy," in U.S. Congress, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Supplemental Reports on Intelligence Activities*, Book VI, S. Rept. 94-755, 94th Cong.,

November 1917 with General Orders No. 64 of the General Headquarters of the American Expeditionary Force.

2nd sess. (Washington: GPO, 1976), pp. 313-352.

During World War II, in addition to the President's order and prevailing armed forces directives on marking and handling classified information, the Office of War Information, in September 1942, issued a government-wide regulation on creating and managing classified materials. Among other ad hoc arrangements of the era, personnel cleared to work on the Manhattan Project for the production of the atomic bomb, in committing themselves not to disclose protected information improperly, were "required to read and sign either the Espionage Act or a special secrecy agreement," establishing their awareness of their secrecy obligations and a fiduciary trust which, if breached, constituted a basis for their dismissal.[3]

A few years after the conclusion of World War II, President Harry S. Truman, in February 1950, issued E.O. 10104, which, while superseding E.O. 8381, basically reiterated its text, but added a fourth "Top Secret" classification designation, making American information security categories consistent with those of our allies. At the time of the promulgation of this order, however, plans were underway for a complete overhaul of the classification program, which would result in a dramatic change in policy.

[3] Anthony Cave Brown and Charles B. MacDonald, eds., *The Secret History of the Atomic Bomb* (New York: Dial Press/James Wade, 1977), p. 201.

E.O. 10290, issued in September 1951, introduced three sweeping innovations in security classification policy. First, the order indicated the Chief Executive was relying upon "the authority vested in me by the Constitution and statutes, and as President of the United States" in issuing the directive. This formula appeared to strengthen the President's discretion to make official secrecy policy: it intertwined his responsibility as Commander in Chief with the constitutional obligation to "take care that the laws be faithfully executed."[4] Second, information was now classified in the interest of "national security," a somewhat new, but nebulous, concept, which, in the view of some, conveyed more latitude for the creation of official secrets. It replaced the heretofore relied upon "national defense" standard for classification. Third, the order extended classification authority to nonmilitary entities, to be exercised by, presumably, but not explicitly limited to, those having some role in "national security" policy.

The broad discretion to create official secrets granted by E.O. 10290 engendered widespread criticism from the public and the press. In response, President Dwight D. Eisenhower, shortly after his election to office, instructed Attorney General Herbert Brownell to review the order with a view to revising or rescinding it. The subsequent recommendation was for a new directive, which was issued in November 1953 as E.O. 10501. It withdrew classification authority from 28 entities, limited this discretion in 17 other units to the agency head, returned to the "national defense" standard for applying secrecy, eliminated the "Restricted" category, which was the lowest level of protection, and explicitly defined the remaining three classification areas to prevent their indiscriminate use.

Thereafter, E.O. 10501, with slight amendment, prescribed operative security classification policy and procedure for the next two decades. Successor orders built on this reform. These

---

[4] In *Environmental Protection Agency* v. *Mink*, Supreme Court Associate Justice Byron White, delivering the majority opinion, proffered that "Congress could certainly have provided that the Executive Branch adopt new procedures" for the security classification of information, "or it could have established its own procedures — subject only to whatever limitations the Executive [or constitutional separation of powers]

included E.O. 11652, issued by President Richard M. Nixon in March 1972, followed by E.O. 12065, promulgated by President Jimmy Carter in June 1978. For 30 years, these classification directives narrowed the bases and discretion for assigning official secrecy to executive branch documents and materials. Then, in April 1982, this trend was reversed with E.O. 12356, issued by President Ronald Reagan. This order expanded the categories of classifiable information, mandated that information falling within these categories be classified, authorized the reclassification of previously declassified documents, admonished classifiers to err on the side of classification, and eliminated automatic declassification arrangements.[5]

---

privilege may be held to impose upon such congressional ordering." 410 U.S. 73, 83 (1973).

[5] See Richard C. Ehlke and Harold C. Relyea, "The Reagan Administration Order on Security Classification: A Critical Assessment," *Federal Bar News & Journal*, vol. 30, Feb. 1983, pp. 91-97.

President William Clinton returned security classification policy and procedure to the reform trend of the Eisenhower, Nixon, and Carter Administrations with E.O. 12958 in April 1995. Adding impetus to the development and issuance of the new order were changing world conditions: the democratization of many eastern European countries, the demise of the Soviet Union, and the end of the Cold War. Accountability and cost considerations were also significant influences. In 1985, the temporary Department of Defense (DOD) Security Review Commission, chaired by retired General Richard G. Stilwell, declared that there were "no verifiable figures as to the amount of classified material produced in DOD and in defense industry each year." Nonetheless, it concluded that "too much information appears to be classified and much at higher levels than is warranted."[6] In October 1993, the cost of the security classification program became clearer when the General Accounting Office (GAO) reported that it was "able to identify government-wide costs directly applicable to national security information totaling over $350 million for 1992." After breaking this figure down — it included only $6 million for declassification work — the report added that "the U.S. government also spends additional billions of dollars annually to safeguard information, personnel, and property."[7] E.O. 12958 set limits for the duration of classification, prohibited the reclassification of properly declassified records, authorized government employees to challenge the

[6] U.S. Department of Defense, Department of Defense Security Review Commission, *Keeping the Nation's Secrets* (Washington: GPO, 1985), pp. 48-49.

[7] U.S. General Accounting Office, *Classified Information: Costs of Protection Are Integrated with Other Security Costs*, GAO Report GAO/NSIAD-94-55 (Washington: Oct. 1993), p. 1.

classification status of records, reestablished the balancing test of E.O. 12065 weighing the need to protect information vis-a-vis the public interest in its disclosure, and created two review panels — one on classification and declassification actions and one to advise on policy and procedure.

Recently, in March 2003, President George W. Bush issued E.O. 13292 amending E.O. 12958. Among the changes made by this directive were adding infrastructure vulnerabilities or capabilities, protection services relating to national security, and weapons of mass destruction to the categories of classifiable information; easing the reclassification of declassified records; postponing the automatic declassification of protected records 25 or more years old, beginning in mid-April 2003 to the end of December 2006; eliminating the requirement that agencies prepare plans for declassifying records; and permitting the Director of Central Intelligence to block declassification actions of the Interagency Security Classification Appeals Panel, unless overruled by the President.

The security classification program has evolved over 65 years. One may not agree with all of its rules and requirements, but, as an expression of policy and procedure, its attention to detail is commendable. The operative presidential directive, as amended, defines its principal terms. Those who are authorized to exercise original classification authority are identified. Exclusive categories of classifiable information are specified, as are the terms of the duration of classification, as well as classification prohibitions and limitations. Classified information is required to be marked appropriately along with the identity of the original classifier, the agency or office of origin, and a date or event for declassification. Authorized holders of classified information who believe that its protected status is improper are "encouraged and expected" to challenge that status through prescribed arrangements. Mandatory declassification reviews are also authorized to determine if protected records merit continued classification at their present level, a lower level, or at all. Unsuccessful classification challenges and mandatory declassification reviews are subject to review by the Interagency Security Classification Appeals Panel. General restrictions on access to classified information are prescribed, as are distribution controls for classified information. An

entity — the Information Security Oversight Office within the National Archives and Records Administration — is mandated to provide central management and oversight of the security classification program. If the director of this entity finds that a violation of the order or its implementing directives has occurred, it must be reported to the head of the agency or to the appropriate senior agency official so that corrective steps, if appropriate, may be taken.

Pseudo-Classification

Not long ago, in the closing days of January, *GCN Update*, the online, electronic news service of *Government Computer News*, reported that "dozens of classified Homeland Security Department documents" had been accidently made available on a public Internet site for several days due to an apparent security glitch at the Department of Energy. Describing the contents of the compromised materials and reactions to the breach, the account stated the "documents were marked 'for official use only,' the lowest secret-level classification." The documents, of course, were not security classified, because the marking cited is not authorized by E.O. 12958. Interestingly, however, in view of the fact that this misinterpretation appeared in a story to which three reporters contributed, perhaps it reflects, to some extent, the current state of confusion about the origin and status of various new information control markings which have appeared of late.[8]

[8] Patience Wait, "DHS Classified Briefings Leaked Through Energy System," *GCN Update*, Jan. 27, 2005, available at [http://www.gcn.com/vol1_no1/daily-updates/34907-1.html]; credited as contributing to this story were GCN staff writers Susan M. Menke and Mary Mosquera.

Moreover, the situation is not unprecedented. In March 1972, a subcommittee of the House Committee on Government Operations, now the House Committee on Government Reform, launched the first oversight hearings on the administration and operation of the Freedom of Information (FOI) Act. Enacted in 1966, the FOI Act had become operative in July 1967. In the early months of 1972, the Nixon Administration was developing new security classification policy and procedure, which would be prescribed in E.O. 11652, issued in early March. The subcommittee's strong interest in this directive is reflected in its unsuccessful attempt to receive testimony from one of the directive's principal architects, David Young, Special Assistant to the National Security Council. The subcommittee sought his testimony as it examined the way in which the new order "will affect the economic and efficient operation of our security classification system, the rationale behind its various provisions, and alternatives to the present approach."[9] Although Young, through White House Counsel John Dean III, declined the invitation to testify, the subcommittee was more successful in obtaining department and agency responses to its August 1971 questionnaire, which, among other questions, asked: "What legend is used by your agency to identify records which are *not* classifiable under Executive Order 10501 [the operative order at the time] but which are not to be made available outside the government?"[10] Of 58 information control markings identified in response to this question, the most common were "For Official Use Only" (11 agencies); "Limited Official Use" (nine agencies); "Official Use Only" (eight agencies); "Restricted Data" (five agencies); "Administratively Restricted" (four agencies); "Formerly Restricted Data" (four agencies); and "Nodis," or no dissemination (four agencies). Seven other markings were used

[9] Letter to David Young, Apr. 24, 1972, appearing in U.S. Congress, House Committee on Government Operations, *U.S. Government Information Policies and Practices — Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7)*, hearings, 92nd Cong., 2nd sess. (Washington: GPO, 1972), pp. 2452-2453.

[10] Ibid., p. 2930 (emphasis in original).

by two agencies in each case.[11] A CRS review of the agency responses to the control markings question prompted the following observation.

> Often no authority is cited for the establishment or origin of these labels; even when some reference is provided it is a handbook, manual, administrative order, or a circular but not statutory authority. Exceptions to this are the Atomic Energy Commission, the Defense Department and the Arms Control and Disarmament Agency. These agencies cite the Atomic Energy Act, N.A.T.O. related laws, and international agreements as a basis for certain additional labels. The Arms Control and Disarmament Agency acknowledged it honored and adopted State and Defense Department labels.[12]

[11] See Ibid., pp. 2933-2934.

[12] Ibid., p. 2932.

At a May 1, 1972, hearing on the relationship of the FOI Act to the security classification system, Chairman William S. Moorhead of the Foreign Operations and Government Information Subcommittee wondered aloud how the act's nine exemptions to the rule of disclosure could be expanded to the multiple information control markings which the departments and agencies had indicated they were using.[13] The following day, when the hearing continued, William D. Blair, Jr., Deputy Assistant Secretary for Public Affairs at the Department of State, explained that some information control markings were used to route otherwise classified information to a limited group of recipients, "those people who have responsibility for the subject matter concerned." He then addressed the relationship question raised by Chairman Moorhead, saying:

> But if a question came in under the Freedom of Information Act or from the Congress or other representative of the public for that given document, the fact that it is marked, let's say, NODIS, is not relevant. What is relevant to the making available of that document to the public is whether or not it was properly classified under the Executive order and whether or not the Freedom of Information Act, for example, once we have reviewed the document, still pertains, whether we feel that the need for the classification still pertains and whether, in fact, we are authorized under the act to withhold it.[14]

A moment thereafter, he explained another marking, which was not applied to route classified information, but apparently had the same effect as a security classification protective marking.

> "Limited official use" is not a fixed distribution channel, such as some of these other terms you have mentioned. It simply is an administrative red flag put on that document which means that the document should be given the same degree of protection, physical protection as a classified document even though it is not, under the Executive order, classifiable.[15]

---

[13] Ibid., p. 2284.

[14] Ibid., pp. 2477-2478.

[15] Ibid., p. 2478.

However, when asked if, in applying this particular marking, "you mean to exclude all individuals outside the Department, subject to the Freedom of Information Act, where they can go to court to obtain it," Blair's response indicated that the use of the marking was somewhat more complicated than functioning as a parallel security label, when he said:

> Not necessarily sir. That may be the case. For instance, one set of files on which we use "Limited official use" quite commonly is personnel files. Well, we would be very likely to deny those personnel files if they were requested by a member of the public, on quite different grounds from classification — on grounds of invasion of privacy. But on the other hand we may use a term like "Limited official use" on an internal advisory document which we may be authorized under the Freedom of Information Act to withhold if it were requested; but we might decide not to claim that authority.[16]

Although an attempt was made to obtain further explanation of how information control markings were used, the questioner, a subcommittee staff member, concluded "that all you have convinced me of is to reinforce my belief that a distribution marking is merely a more restrictive or stricter type of classification marking."[17]

Later in the hearing, in an exchange with the subcommittee's staff director, DOD General Counsel J. Fred Buzhardt made another attempt to clarify the use of control markings.

> In the first place, you have a determination as to whether the material is to be classified. Once the decision is made that the information should be classified, then the limitation of access has to do with the protection of that which is classified. We also have the responsibility to control the dissemination. That is what these access limitations are for, to control dissemination, to confine

[16] Ibid.

[17] Ibid., p. 2479.

> access to the people who have a need to know to work with the information. It is a protection device. We must use protective devices of some sort.[18]

Asked if the control markings, such as "eyes only," were applied to material that was not classified, Buzhardt said:

> I presume you wouldn't find "eyes only" in an authorized way upon any document that was not classified by one of the classifiers. Once it is classified you can use limitations on distribution to protect it. That is a protective device.[19]

To this response, Blair added:

[18] Ibid., p. 2497.

[19] Ibid.

> The purpose of classification is to determine what information is or is not available to the public outside of the government. These labels that you are referring to have nothing to do with that. They have absolutely no value for determining what information or what document may be given to a member of the public. They are simply a mailing device, if you like, a means by which a superior determines which of his subordinates he wishes to deal with this particular matter and be aware of this particular information.[20]

These explanations of information control markings being used as devices to limit the distribution of classified information within DOD and the State Department, however, did not appear to extend to all such markings. Blair, for instance, had testified that the "Limited official use" marking was applied, in his words, "quite commonly" to personnel files, which, for the most part, were not security classifiable materials at that time. Several entities indicating they used information control markings had no original classification authority. These included, among others, the American Revolution Bicentennial Commission (ARBC), the Department of Housing and Urban Development, and the Federal Trade Commission (FTC).[21] Does this situation mean that the control markings of these entities were applied only to limit the distribution of classified information received from other agencies? That is possible, but seems unlikely. The ARBC control marking, "Administratively confidential," appears to have been designed for information of a different character from national security classified materials, while the FTC label, "For staff use only," does not appear to have provided much limitation on the distribution of classified information.

Before this phase of the oversight hearings on the FOI Act concluded, the subcommittee received testimony from Assistant Attorney General Ralph E. Erickson of the Office of Legal

---

[20] Ibid., pp. 2497-2498.

[21] See Ibid., p. 2935.

Counsel, Department of Justice, on May 11, 1972. During the course of his appearance before the subcommittee to discuss E.O. 11652, the use of control markings to limit the distribution of classified information was raised with the following question from the subcommittee's staff director.

> Can you assure us today that these kinds of distribution access stamps will not be used on unclassified material in any Executive agency or department? If you can guarantee that, then I will go along and say [Section] 4(a) is a big improvement. But I do not think that is going to be the case from other testimony we have had. I think people are going to substitute LIMDIS, NODIS, and all these other stamps for the stamps authorized under the Executive order and we are going to proliferate more and more and more.[22]

Erickson offered a two part response.

> First, it is our hope within the Department of Justice and I think in other agencies, too, that the use of this sort of a restricted distribution will be severely limited or removed. But, more importantly, it [Section 4(a)] specifically limits the use of such designations to the point where they must conform with the provision of this order and would have no effect in terms of classification. It will not prevent the information from otherwise being made available. It may in part restrict the distribution within the department but certainly if a request were made under the Freedom of Information Act it has no applicability.[23]

He assured his questioner that control markings used to limit the distribution of classified information "will not have any effect on disclosure" under the FOI Act, and would not, in themselves, be a bar to disclosure.

---

[22] Ibid., pp. 2705-2706.

[23] Ibid., p. 2706.

Later, in May 1973, when reviewing this phase of the subcommittee's oversight hearings, a report by the parent Committee on Government Operations commented:

> One of the difficult problems related to the effective operation of the security classification system has been the widespread use of dozens of special access, distribution, or control labels, stamps, or markings on both classified and unclassified documents. Such control markings were not specifically authorized in Executive Order 10501, but have been utilized for many years by many executive agencies having classification authority and dozens of other agencies who do not possess such authority. The use of such stamps has, in effect, been legitimized in section 9 of the new Executive Order 11652.[24]

On this matter, the report concluded that, "while there is a clear rationale for the use of such access or control markings, the basic problem is the effect of the proliferation of their use on the effective operation of the classification system. This problem," it continued, "fully explored with executive branch witnesses during the hearings, is one that this committee believes should be carefully monitored by the [newly created] Interagency Classification Review Committee and by department heads to assure that it does not interfere with the overall effectiveness and integrity of the classification system."[25]

That such interference with the security classification program by these types of information control markings — in terms of both their confusion and presumed coequal authority with classification markings — has occurred in the post-9/11 environment may be discerned in the recent *GCN Update* story cited earlier. In some instances, the phraseology of the markings is new, and, in at least one case, the asserted authority for the label is, unlike most of those of the past, statutory.

---

[24] U.S. Congress, House Committee on Government Operations, *Executive Classification of Information — Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act (5 U.S.C. 552)*, H. Rept. 93-221, 93rd Cong., 2nd sess. (Washington: GPO, 1973), p. 75.

[25] Ibid., p. 78.

Among the problems they generate, however, the one identified over three decades ago by the House Committee on Government Operations endures.

Broadly considering the contemporary situation regarding information control markings, a recent information security report by the JASON Program Office of the MITRE Corporation proffered the following assessment.

> The status of sensitive information outside of the present classification system is murkier than ever. ... "Sensitive but unclassified" data is increasingly defined by the eye of the beholder. Lacking in definition, it is correspondingly lacking in policies and procedures for protecting (or not protecting) it, and regarding how and by whom it is generated and used.[26]

A contemporaneous Heritage Foundation report appeared to agree with this appraisal, saying:

> The process for classifying secret information in the federal government is disciplined and explicit. The same cannot be said for unclassified but security-related information for which there is no usable definition, no common understanding about how to control it, no agreement on what significance it has for U.S. national security, and no means for adjudicating concerns regarding appropriate levels of protection.[27]

Concerning the current "Sensitive But Unclassified" (SBU) marking, a recent report by the Federal Research Division of the Library of Congress commented that guidelines for its use are needed, and noted that "a uniform legal definition or set of procedures applicable to all Federal government agencies does not now exist." Indeed, the report indicates that SBU has been utilized in different contexts with little precision as to its scope or meaning, and, to add a bit of chaos to an already confusing situation, is "often referred to as Sensitive Homeland Security Information."[28]

---

[26] MITRE Corporation, JASON Program Office, *Horizontal Integration: Broader Access Models for Realizing Information Dominance* (McLean, VA: Dec. 2004), p. 5.

[27] Carafano and Heyman, "DHS 2.0: Rethinking the Department of Homeland Security," p. 20.

[28] U.S. Library of Congress, Federal Research Division, *Laws and Regulations Governing the Protection of Sensitive But Unclassified Information*, by Alice R. Buchalter, John Gibbs, and Marieke Lewis (Washington: Sept. 2004), p. i.

Assessments of the variety and management of information control markings, other than those prescribed for the classification of national security information, are underway at CRS and GAO. Early indications are that very little of the attention to detail that attends the security classification program is to be found in other information control marking activities. Key terms often lack definition. Vagueness exists regarding who is authorized to applying markings, for what reasons, and for how long. Uncertainty prevails concerning who is authorized to remove markings and for what reasons.

One Congressional Response

Half a century ago, in November 1954, Secretary of Commerce Sinclair Weeks announced that, at the direction of the President and on the recommendation of the National Security Council, he was creating an Office of Strategic Information (OSI) within his department. The mission of this new entity, according to the Secretary, was to work with various private sector organizations "in voluntary efforts to prevent unclassified strategic data from being made available to those foreign nations which might use such data in a manner harmful to the defense interests of the United States."[29] The new office, however, was something of an anomaly. It had no legislative charter, and its activities, in many regards, appeared to overlap with, and duplicate, certain more clearly stated functions of other agencies. Because the concept of "strategic information" was not precisely defined, its regulatory application was seen as potentially sweeping more broadly than the protections established for the classification of national security information. Nonetheless, the OSI was created to detect any imbalance favoring the Communist bloc in exchanges of scientific, technical, and economic information, and to alert federal agencies, as well as scientists, businesses,

[29] U.S. Department of Commerce, Office of the Secretary, *Press release (G-520)* (Washington: Nov. 5, 1954); James Russell Wiggins, *Freedom or Secrecy*, Revised edition (New York: Oxford University Press, 1964), pp. 102-103.

and the press to the indiscriminate publication of unclassified information of possible benefit to an enemy nation.

Journalists and scientists took their objections to the OSI to a House subcommittee studying government information policy and practice.[30] Having serious reservations about the OSI, the subcommittee urged its abolition, a recommendation endorsed by the parent Committee on Government Operations (now known as the Committee on Government Reform).[31] In April 1957, the House eliminated all funds for the OSI and prohibited the transfer of any money from other sources for its continuation.[32] When the Senate agreed to this action, Secretary Weeks was forced to abolish the OSI.[33] With the demise of the office went a vague concept of information control which had strong potential, in its application, for sweeping beyond carefully crafted security classification protections and otherwise complicating their comprehension and legitimacy.

While current department and agency use of vaguely defined information control marking with weak and, in some regards, nebulous management regimes, would seemingly not warrant the drastic action taken in the case of OSI, other options are available. These might include a circumscribed and particularized legislative authorization for some such marking(s), or a legislative limitation or restriction of the use of such markings.

Thank you for your attention. I welcome your questions.

---

[30] U.S. Congress, House Committee on Government Operations, *Availability of Information from Federal Departments and Agencies*, hearings, 84th Cong., 2nd sess. (Washington: GPO, 1956), pp. 1123-1187, 1233-1286, 1447-1521, 1639-1711.

[31] U.S. Congress, House Committee on Government Operations, *Availability of Information from Federal Departments and Agencies*, H. Rept. 2947, 84th Cong., 2nd sess. (Washington: GPO, 1956), p. 91.

[32] *Congressional Record*, vol. 103, Apr. 9, 1957, p. 5376; also see U.S. Congress, House Committee on Government Operations, *Availability of Information from Federal Departments and Agencies*, H. Rept. 2578, 85th Cong., 2nd sess. (Washington: GPO, 1958), pp. 13-14.

[33] *Federal Register*, vol. 22, July 24, 1957, p. 5876.

Biographical Profile

Harold C. Relyea is a Specialist in American National Government with the Congressional Research Service (CRS) of the Library of Congress. A member of the CRS staff since 1971, he has held both managerial and research positions during his career. His principal areas of research responsibility include the presidential office and powers, executive branch organization and management, executive-congressional relations, congressional oversight, and various aspects of government information policy and practice. He has testified before congressional panels on various occasions, and has served as an expert resource for other organizations. In addition to his CRS duties, Dr. Relyea has authored numerous articles for scholarly and professional publications in the United States and abroad. Currently preparing a book on national emergency powers, his recently published titles include *Silencing Science: National Security Controls and Scientific Communication* (1994), *Federal Information Policies in the 1990s* (1996), *The Executive Office of the President* (1997), and *United States Government Information: Policies and Sources* (2002). He serves on the editorial board of *Government Information Quarterly*, the *International Journal of Electronic Government Research*, and the *Journal of E-Government*, and has held similar positions with several other journals in the past. He is also a member of the Advisory and Development Board of the College of Information Studies of the University of Maryland. An undergraduate of Drew University, he received his doctoral degree in government from The American University.